

# **RANDOM-NUMBER GENERATING CIRCUIT, NONCONTACT IC CARD AND READER/WRITER HAVING SAME RANDOM-NUMBER GENERATING CIRCUIT INSIDE, AND METHOD FOR TESTING DEVICE HAVING SAME RANDOM-NUMBER GENERATING CIRCUIT INSIDE**

**Publication number:** JP2000222176

**Publication date:** 2000-08-11

**Inventor:** FUJIOKA SOZO

**Applicant:** MITSUBISHI ELECTRIC CORP; MITSUBISHI DENKI  
SYS LSI DES

**Classification:**


- **International:** G06K19/10; G06F1/02; G06F7/58; G06K17/00;  
G09C1/00; G06K19/10; G06F1/02; G06F7/58;  
G06K17/00; G09C1/00; (IPC1-7): G06F7/58;  
G06K17/00; G06K19/10; G09C1/00

- **European:** G06F7/58P1

**Application number:** JP19990026369 19990203

**Priority number(s):** JP19990026369 19990203

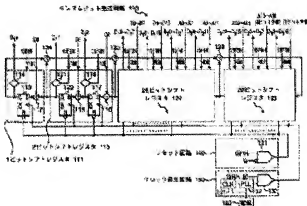
**Also published as:**

 US 6480869 (B1)

Report a data error here

**Abstract of JP2000222176**

**PROBLEM TO BE SOLVED:** To generate random number data which are irregular and hardly predicted and to generate the random number data fast with simple constitution by generating the random number data by making use of bit data sent through an external signal line. **SOLUTION:** A random-bit generating circuit 110 adds bit data which changes with time according to process contents to be executed by a CPU to respective bit data stored in a 1-bit shift register 111, a 2-bit shift register 115, a 25-bit shift register 122, and a 20-bit shift register 123 constituting what is called a 48-bit M-series random number generating circuit. Namely, the respective bit data A0 to A19 of a 20-bit address signal sent through a system bus, the respective bit data D0 to D15 of a 16-bit data signal, and the respective bit data of 12 bits in total composed of other signals are added respectively. The 3 bytes obtained by the addition, i.e., data D10 to D15, D20 to D215, and D30 to D316 of 48 bits in total are outputted as random number data.



Data supplied from the **esp@cenet** database - Worldwide

(19)日本特許庁(JP)

(12) 公開特許公報(A)

(11)特許出願公開番号

特開2000-222176  
(P2000-222176A)

(43)公開日 平成12年8月11日(2000.8.11)

| (51)Int.Cl. <sup>7</sup> | 識別記号  | F I           | テモット <sup>7</sup> (参考) |
|--------------------------|-------|---------------|------------------------|
| G 0 6 F 7/58             |       | C 0 6 F 7/58  | A 5 B 0 3 J            |
| G 0 6 K 17/00            |       | C 0 6 K 17/00 | T 5 B 0 5 8            |
| 19/10                    |       | G 0 9 C 1/00  | 6 5 0 B 5 J 1 0 4      |
| G 0 9 C 1/00             | 6 5 0 | C 0 6 K 19/00 | R 9 A 0 0 1            |

審査請求 未請求 請求項の数7 O L (全 13 頁)

(21)出願番号 特願平11-26369

(22)出願日 平成11年2月3日(1999.2.3)

(71)出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(71)出願人 391024515

三菱電機システムエル・エス・アイ・デザ  
イン株式会社

兵庫県伊丹市中央3丁目1番17号

(72)発明者 藤岡 宗三

兵庫県伊丹市中央3丁目1番17号 三菱電  
機システムエル・エス・アイ・デザイン株  
式会社内

(74)代理人 100062144

弁理士 青山 薫 (外2名)

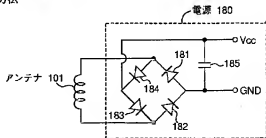
最終頁に続く

(54)【発明の名称】 乱数生成回路、当該乱数生成回路を内蔵する非接触 I Cカード及びリーダ/ライタ、並びに、当該乱数生成回路を内蔵する装置のテスト方法

(57)【要約】

【課題】 簡単な構成で、かつ、高速に精度の高い乱数を発生する乱数生成回路を提供する。

【解決手段】 本発明の乱数生成回路は、カスケード接続された1以上のビットのクロック同期型シフトレジスタと、上記複数のシフトレジスタの内の少なくとも1組のシフトレジスタの出力の合計を求め、求めた合計のデータを所定のシフトレジスタの入力端子に入力する加算回路と、上記各シフトレジスタにクロック信号を入力するクロック発生回路とで構成される乱数生成回路であって、上記複数のシフトレジスタの内の1以上のシフトレジスタは、格納しているビットデータの内の1以上のビットデータに外部信号線に流れるビットデータを加算する加算手段と、上記加算手段による加算後に、格納しているビットデータの内の1以上の所定のビットデータを乱数データとして出力する出力手段とを備えることを特徴とする。



## 【特許請求の範囲】

【請求項1】 カスケード接続された複数のクロック同期型シフトレジスタと、上記複数のシフトレジスタの内の2以上のシフトレジスタの出力の合計を求め、求めた合計のデータを初段のシフトレジスタの入力端子に入力する回路と、上記各シフトレジスタにクロック信号を入力するクロック発生回路とを備え、各シフトレジスタの出力するビットデータを乱数データとして出力する乱数生成回路であって、

上記複数のシフトレジスタの内の1以上のシフトレジスタは、外部信号入力端子と、格納しているビットデータの内の1以上のビットデータに上記外部信号入力端子を介して入力されるビットデータを加算する加算回路とを備え、加算回路による加算後のビットデータを乱数データとして出力することを特徴とする乱数生成回路。

【請求項2】 カスケード接続された複数のクロック同期型シフトレジスタと、上記複数のシフトレジスタの内の2以上のシフトレジスタの出力の合計を求め、求めた合計のデータを初段のシフトレジスタの入力端子に入力する回路と、上記各シフトレジスタにクロック信号を入力するクロック発生回路とを備え、各シフトレジスタの出力するビットデータを乱数データとして出力する乱数生成回路であって、

上記クロック発生回路は、所定の周波数のクロック信号を生成するCLK回路と、上記CLK回路により生成されたクロック信号を基準周波数信号として受け取るPLL回路とで構成され、上記PLL回路の出力を上記各シフトレジスタに出力することを特徴とする乱数生成回路。

【請求項3】 請求項1又は請求項2に記載の乱数生成回路において、

上記シフトレジスタを構成するクロック同期型のフリップフロップは、電源投入時に出力するデータを“H”とする第1構成要素と、第1構成要素と同一のドライブ能力を有し、電源投入時に出力するデータを“L”とする第2構成要素とを備え、上記第1及び第2構成要素の出力端子には、それぞれ同一の容量の配線及びトランジスタが接続されていることを特徴とする乱数生成回路。

【請求項4】 請求項1乃至請求項3の何れかに記載の乱数生成回路において、

更に、リセット要求信号の入力に応じて各シフトレジスタにリセット信号を出力するリセット回路を備え、上記クロック発生回路は、クロック停止信号の入力に応じてクロック信号の各シフトレジスタへの出力を停止し、クロック動作信号の入力に応じてクロック信号を各シフトレジスタへ出力する論理回路を備えることを特徴とする乱数生成回路。

【請求項5】 請求項1乃至請求項4の何れかに記載の乱数生成回路を内蔵する非接触ICカードであって、当該非接触ICカード用リーダ/ライタとの間で、上記内

蔵する乱数生成回路から出力される乱数データを用いて通信処理を実行する制御手段を備え、上記制御手段により使用される所定の信号線が上記外部信号入力端子に接続されていることを特徴とする非接触ICカード。

【請求項6】 請求項1乃至請求項4の何れかに記載の乱数生成回路を内蔵する非接触ICカード用リーダ/ライタであって、対応する非接触ICカードとの間で、上記内蔵する乱数生成回路から出力される乱数データを用いて通信処理を実行する制御手段を備え、上記制御手段により使用される所定の信号線が上記外部信号入力端子に接続されていることを特徴とする非接触ICカード用リーダ/ライタ。

【請求項7】 請求項4に記載の乱数生成回路を内蔵し、当該内蔵する乱数生成回路から出力される乱数データを用いて所定の処理を実行する制御手段を備え、上記制御手段により使用される所定の信号線が上記外部信号入力端子に接続されている装置のテスト方法であって、クロック発生回路から所定の周波数のクロック信号が出力されている状態において、クロック発生回路の論理回路にクロック停止信号を出力し、リセット回路にリセット要求信号を出力した後に、クロック発生回路の論理回路にクロック動作信号を出力すると同時に上記装置のテスト処理を実行し、上記テスト処理の完了と同時にクロック発生回路の論理回路にクロック停止信号を出力し、出力手段より出力される乱数データの値を読み取り、読み取った乱数データと基準データとの比較により、システムの異常検出を行うことを特徴とする装置のテスト方法。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、乱数生成回路、特に、非接触ICカード及び当該非接触ICカードのリーダ/ライタに用いる乱数生成回路に関する。

## 【0002】

【従来の技術】近年、インテリジェント機能や書き換え可能なメモリ機能を備える薄型の非接触ICカードが数多く提供されている。非接触ICカードは、リーダ/ライタに接続させることなくデータのやり取りができることを特徴とする。非接触ICカードは、例えば、プリペイドカード、ドアの鍵、電車やバスなどの定期券、スキーマのリフト券等に用いられる。

【0003】非接触ICカードに書き込まれているデータの不正流出や改竄を防止するため、上記非接触ICカードと当該カードのリーダ/ライタは、データのやり取りを行う前に、互いを認証する処理を実行する。リーダ/ライタは、自己の発信するボーリング信号に対して所定のレスポンス信号を返信してきた非接触ICカードとの間で相互認証処理を実行する。相互認証処理の方法としては、暗号化鍵を用いる方法が知られている。

【0004】以下、非接触ICカードとリーダ/ライタ

との間で行う暗号を用いた相互認証処理について簡単に説明する。まず、リーダー/ライタは、非接触ICカードに対して内部で生成した乱数aを送信する。非接触ICカードは、受信した乱数aを自己の暗号化鍵を用いて乱数Aに変換し、乱数Aをリーダー/ライタに返送する。リーダー/ライタでは、特定の非接触ICカードとの間で用いる共通の暗号化鍵を用いて上記生成した乱数aを処理して乱数A'を求め、求めた乱数A'と上記非接触ICカードから返送されてきた乱数Aとを比較する。リーダー/ライタは、乱数Aと乱数A'が一致する場合に当該非接触ICカードを正規のものであると認証する。

【0005】次に、非接触ICカードはリーダー/ライタに対して内部で生成した乱数bを送信する。この場合、リーダー/ライタは、受信した乱数bを自己の暗号化鍵を用いて乱数Bに変換し、乱数Bを非接触ICカードに返送する。非接触ICカードは、特定のリーダー/ライタとの間で用いる共通の暗号化鍵を用いて上記生成した乱数bを処理して乱数B'を求め、求めた乱数B'と上記リーダー/ライタから返送されてきた乱数Bとを比較する。非接触ICカードは、乱数Bと乱数B'が一致する場合に当該リーダー/ライタを正規のものであると認証する。

【0006】非接触ICカードおよびリーダー/ライタ内には上記相互認証処理で用いる乱数を生成する乱数生成回路が内蔵されている。図10は、従来より用いられている乱数生成回路500の回路図である。乱数生成回路500は、いわゆる48ビットM系列乱数生成回路と呼ばれる回路であり、カスケード(多段直列)接続された1ビットシフトレジスタ501、2ビットシフトレジスタ504、25ビットシフトレジスタ505及び20ビットシフトレジスタ506、並びに、各ビットシフトレジスタの出力の合計を初段の20ビットシフトレジスタ506の入力端子に入力する加算回路を構成する加算器507、508及び509で構成される。

【0007】1ビットシフトレジスタ501は、CLK回路510より出力されるクロック信号CLKに同期して動作するフリップフロップ502及びトランスファゲート503により構成される。図示しないCPUによりアドレス02EHが選択されたアドレス信号線が“L”から“H”に切り換わった時にフリップフロップ502の出力を乱数データD<sub>1</sub>0として出力する。

【0008】2ビットシフトレジスタ504、25ビットシフトレジスタ505及び20ビットシフトレジスタ506の回路は、各シャフトするビット数だけ上記1ビットシフトレジスタ501と同じ回路を直列に接続したものである。2ビットシフトレジスタ504は、アドレス15FHが選択された時に乱数データD<sub>1</sub>1、D<sub>1</sub>2を出力する。25ビットシフトレジスタ505は、アドレス15FH、15F3H、15F4H及び15F5Hが選択された時に乱数データD<sub>1</sub>3～D<sub>1</sub>7、D<sub>1</sub>8～D<sub>1</sub>15、D<sub>1</sub>0～D<sub>1</sub>7及びD<sub>1</sub>8～D<sub>1</sub>11を出力す

る。20ビットシフトレジスタ506は、アドレス15FH、15F6H及び15F7Hが選択された時に乱数データD<sub>2</sub>12～D<sub>2</sub>15、D<sub>2</sub>0～D<sub>2</sub>7、D<sub>2</sub>8～D<sub>2</sub>15を出力する。

【0009】

【発明が解決しようとする課題】上記構成の乱数生成回路500の生成する乱数は、一定の周期で繰り返す所定の生成パターンを有する。このため、リーダー/ライタと非接触ICカードとの間でやり取りされる通信データが盗聴され、乱数の生成パターンが特定される場合がある。このように乱数の生成パターンが特定されると、暗号化鍵や暗号化処理の内容が解らずとも、乱数aと乱数Aを対応づけたテーブルを用いることで非接触ICカードを偽造することができる。同様に、乱数bと乱数Bを対応づけたテーブルを用いることでリーダー/ライタの偽造を行うことができる。

【0010】上記通信データの盗聴による非接触ICカードやリーダー/ライタの偽造を有効に防止するには、通信データを盗聴しても生成パターンを解読できない程の高度な乱数生成回路が要求される。しかし、乱数生成回路を複雑化すれば乱数生成パターンの不正な解読を有効に防止することができるが、回路のサイズが大きくなってしまふ。特に非接触ICカードの場合、内蔵する乱数生成回路のサイズは小さいほうが好ましい。

【0011】非接触ICカードは、リーダー/ライタと通信可能な領域にある間に相互認証処理を含む通信処理を完了する必要がある。このため、スロットに差し込んで使用するICカードよりも高速な通信処理の実行が要求される。また、非接触ICカードの場合、リーダー/ライタと通信可能な領域内に同時に複数の非接触ICカードが入り込むことがある。この場合、各非接触ICカードは、上記相互認証処理を含む通信処理の実行前に、例えば内部で生成した乱数に基づくタイミングでリーダー/ライタからのポーリング信号に対するレスポンス信号を出力する等、他の非接触ICカードから出力されるレスポンス信号との衝突を回避する処理を実行する必要がある。非接触ICカードとリーダー/ライタ間の通信速度を向上するには、高速で動作する乱数生成回路が要求される。

【0012】本発明は、簡単な構成で当該回路を内蔵する装置の小型化に寄与し、かつ、高速に規則性の無い予測の困難な乱数データを発生する乱数生成回路、当該乱数生成回路を内蔵する非接触ICカード、及び、当該乱数生成回路を内蔵する非接触ICカード用リーダー/ライタを提供することを目的とする。

【0013】

【課題を解決するための手段】本発明の第1の乱数生成回路は、カスケード接続された複数のクロック同期型シフトレジスタと、上記複数のシフトレジスタの内の2以上のシフトレジスタの出力の合計を求め、求めた合計の

データを初段のシフトレジスタの入力端子に入力する回路と、上記各シフトレジスタにクロック信号を入力するクロック発生回路とを備え、各シフトレジスタの出力するビットデータを乱数データとして出力する乱数生成回路であって、上記複数のシフトレジスタの内の1以上のシフトレジスタは、外部信号入力端子と、格納しているビットデータの内の1以上のビットデータに上記外部信号入力端子を介して入力されるビットデータを加算する加算回路とを備え、加算回路による加算後のビットデータを乱数データとして出力することを特徴とする。

【0014】本発明の第2の乱数生成回路は、カスケード接続された複数のクロック同期型シフトレジスタと、上記複数のシフトレジスタの内の2以上のシフトレジスタの出力の合計を求め、求めた合計のデータを初段のシフトレジスタの入力端子に入力する回路と、上記各シフトレジスタにクロック信号を入力するクロック発生回路とを備え、各シフトレジスタの出力するビットデータを乱数データとして出力する乱数生成回路であって、上記クロック発生回路は、所定の周波数のクロック信号を生成するCLK回路と、上記CLK回路により生成されたクロック信号を基準周波数信号として受け取るPLL回路とで構成され、上記PLL回路の出力を上記各シフトレジスタに出力することを特徴とする。

【0015】本発明の第3の乱数生成回路は、上記第1又は第2の乱数生成回路において、上記シフトレジスタを構成するクロック同期型のフリップフロップは、電源投入時に出力するデータを“H”とする第1構成要素と、第1構成要素と同一のドライブ能力を有し電源投入時に出力するデータを“L”とする第2構成要素とを備え、上記第1及び第2構成要素の出力端子には、それぞれ同一の容量の配線及びトランジスタが接続されていることを特徴とする。

【0016】本発明の第4の乱数生成回路は、上記第1乃至第3の何れかの乱数生成回路において、更に、リセット要求信号の入力に応じて各シフトレジスタにリセット信号を出力するリセット回路を備え、上記クロック発生回路は、クロック停止信号の入力に応じてクロック信号の各シフトレジスタへの出力を停止し、クロック動作信号の入力に応じてクロック信号を各シフトレジスタへ出力する論理回路を備えることを特徴とする。

【0017】本発明の非接触ICカードは、上記第1乃至第4の何れかの乱数生成回路を内蔵する非接触ICカードであって、当該非接触ICカード用リーダ/ライタとの間で、上記内蔵する乱数生成回路から出力される乱数データを用いて通信処理を実行する制御手段を備え、上記制御手段により使用される所定の信号線が上記外部信号入力端子に接続されていることを特徴とする。

【0018】本発明のリーダ/ライタは、上記第1乃至第4の何れかの乱数生成回路を内蔵する、非接触ICカード用リーダ/ライタであって、対応する非接触ICカ

ードとの間で、上記内蔵する乱数生成回路から出力される乱数データを用いて通信処理を実行する制御手段を備え、上記制御手段により使用される所定の信号線が上記外部信号入力端子に接続されていることを特徴とする。

【0019】上記第4の乱数生成回路を内蔵し、当該内蔵する乱数生成回路から出力される乱数データを用いて所定の処理を実行する制御手段を備え、上記制御手段により使用される所定の信号線が上記外部信号入力端子に接続されている装置のテスト方法であって、クロック発生回路の論理回路にクロック停止信号を出力すると共に、リセット回路にリセット要求信号を出力した後に、クロック発生回路の論理回路にクロック動作信号を出力すると同時に上記装置のテスト処理を実行し、上記テスト処理の完了と同時にクロック発生回路の論理回路にクロック停止信号を出力し、出力手続より出力される乱数データの値を読み取り、読み取った乱数データと基準データとの比較により、システムの異常検出を行い、上記内蔵する乱数生成回路をテスト回路として利用する。これにより、テスト専用の回路を不要にして装置の小型化を図ることができる。

【0020】

【発明の実施の形態】以下、実施の形態に係る乱数生成回路、当該乱数生成回路を内蔵する非接触ICカード、及び、当該乱数生成回路を内蔵する非接触ICカード用リーダ/ライタについて、添付の図面を参照しつつ説明する。

【0021】(1) 非接触ICカード

本実施の形態に係る乱数生成回路を内蔵する非接触ICカードは、例えば、地下鉄の自動改札システムに採用することを想定している。より具体的には、図1に示すように、自動改札機として機能するリーダ/ライタ400の前を、例えば定期券や回数券としての機能を有する非接触ICカード100、200、300を有する人が順に通過する場合を想定する。リーダ/ライタ400は、前を通過する際に通信エリア内に入る非接触ICカード100、200、300を順に認識し、定期券や回数券の種類についての情報、カードが定期券の場合には有効期限などの情報、及び、カードが回数券の場合には残りの枚数などの情報を読み取り、更に、必要に応じて各カードの情報を更新する。

【0022】(2) 非接触ICカードの認証

リーダ/ライタ400は、自己の発信するボーリング信号に対して所定のレスポンス信号を返信してきた非接触ICカードとの間で相互認証処理を実行する。図2は、非接触ICカード100とリーダ/ライタ400との間で行われる相互認証処理のシーケンスを示す図である。まず、リーダ/ライタ400から非接触ICカード100に対して内蔵する乱数生成回路により生成した認証用乱数aを送信する(ステップS1)。通信エリア内において認証用乱数aを受信した非接触ICカード100

は、自己の暗号化鍵を用いて乱数aを乱数Aに変換し、乱数Aをリーダー/ライター400に対して返信すると共に、内蔵する乱数生成回路により生成した認証用乱数bを送信する(ステップS2)。リーダー/ライター400は、アクセスを行う非接触ICカードと共通に用いる暗号化鍵を用いて乱数aを乱数A'に変換し、乱数A'と非接触ICカード100から返信されてきた乱数Aとが一致する場合に非接触ICカード100を認証する。また、非接触ICカード100より送信されてきた乱数bを自己の暗号化鍵を用いて乱数Bに変換し、乱数Bを非接触ICカード100に対して返信する(ステップS3)。非接触ICカード100は、アクセスを行うリーダー/ライターと共通に用いる暗号化鍵を用いて乱数bを乱数B'に変換し、乱数B'と返信されてきた乱数Bとが一致する場合にリーダー/ライター400を認証する(ステップS4)。

【0023】(3)非接触ICカード及びリーダー/ライターの構成

図3は、非接触ICカード100及びリーダー/ライター400のブロック構成図である。なお、非接触ICカード200、300の構成は、非接触ICカード100と同じであり、重複した説明は省略する。

【0024】非接触ICカード100は、電池レスタイプの非接触ICカードである。電源回路180は、リーダー/ライター400から送信される高周波信号をアンテナ101により受信し、受信した高周波信号を整流して得られる信号を電圧Vccの供給信号としてクロック発生回路130を含む各内部回路に供給する。電源回路180の構成については後に説明する。

【0025】クロック発生回路130は、上記電源回路180から供給される電圧Vccから送られてくるクロック信号CLKを中央演算処理装置であるCPU103、乱数生成回路107を構成するランダムビット生成回路110、及び、その他の回路素子に出力する。クロック発生回路130の構成については後に説明する。

【0026】CPU103には、システムバス170を介して送受信回路102、ROM104、RAM105、情報記憶部106、及び、乱数生成回路107が接続されている。送受信回路102は、アンテナ101に接続されており、CPU103から送られてくる命令やデータを載せた高周波信号をアンテナ101を介して外部に発信すると共に、アンテナ101を介して受信した高周波信号から命令やデータを抽出してCPU103に出力する処理を行う。ROM104は、リーダー/ライター400との相互認証処理等の通信処理を実行するプログラムを格納する。RAM105は、ROM104に格納するプログラムのCPU103による実行時に使用される。情報記憶部106は、独自の情報、例えば非接触ICカード100が定期券として機能する場合、カードの有効期限や有効乗車エリアなどの固有の情報を保持す

る。CPU103は、リーダー/ライター400との通信処理の実行に伴い、必要に応じて上記情報記憶部106に記憶する情報の更新を行う。乱数生成回路107は、CPU103による所定のアドレスの選択に応じてリーダー/ライター400との相互認証処理等で用いる乱数データを上記CPU103に出力する。

【0027】乱数生成回路107は、デコーダ108、ランダムビット生成回路110及びリセット回路140で構成される。デコーダ108は、CPU103のシステムバス170を介して入力されるアドレス信号のデータをデコードしてランダムビット生成回路110に出力する。ランダムビット生成回路110は、システムバス170に流れるアドレス信号のデータ、データ信号のデータ及びその他の信号のデータが内部で生成する乱数データを複雑化するために入力され、上記デコーダ108を介して所定のアドレスの選択された場合に合計で3バイト(48ビット)の乱数データをCPU103に出力する。リセット回路140は、CPU103の制御に応じて所定のリセット信号をランダムビット生成回路140に出力する。なお、ランダムビット生成回路110及びリセット回路140の構成については後に詳しく説明する。

【0028】リーダー/ライター400は、アンテナ401、上記アンテナ401を用いて命令やデータが載った高周波信号の送受信を行う送受信回路402、中央演算処理装置であるCPU403、上記非接触ICカード100との相互認証処理を含む通信プログラムを格納しているROM404、CPU403によるプログラム実行時に使用されるRAM405、インターフェース406、及び、乱数生成回路407より構成される。なお、乱数生成回路407は、非接触ICカード100に内蔵する乱数生成回路107と同じ構成である。

【0029】リーダー/ライター400において、中央演算処理装置であるCPU403は、システムバスを介して送受信回路402、ROM404、RAM405、インターフェース406及び乱数生成回路407に接続されている。送受信回路402は、接続されるアンテナ401を介して受信した高周波信号から命令やデータを抽出してCPU403に出力すると共に、CPU403からの命令やデータを載せた高周波信号をアンテナ401を介して発信する。CPU403は、例えば非接触ICカード100との相互認証処理の実行時に、乱数生成回路407から得られる乱数データを用いる。CPU403は、通信処理の結果をインターフェース406を介して各処理装置へ出力する。

【0030】図4は、電源回路180の構成を示す図である。電源回路180は、整流回路を構成するダイオード181、182、183及び184、並びに、容量185で構成される。当該整流回路は、アンテナ101を介して入力される高周波信号の整流を行い、当該整流後

の信号を電圧供給信号として各内部回路に出力する。

【0031】図5は、リーダー/ライター400からの高周波信号の受信開始から電源回路180から出力される電圧供給信号の電位の変化を示すグラフである。図示するように、電源回路180から出力される電圧供給信号の電位が規定値Vccになるには、高周波信号の受信を開始してから所定の時間が必要である。なお、電圧供給信号の電位がVccとなるまでに要する時間は、リーダー/ライター400との通信環境により変化する。

【0032】(4) 乱数生成回路

図6は、乱数生成回路107に内蔵されるランダムビット生成回路110及びリセット回路140、並びに、クロック発生回路130の詳細な構成を示す図である。

【0033】(4-1)ランダムビット生成回路

ランダムビット生成回路110は、いわゆる48ビットM系列乱数生成回路を構成する1ビットシフトレジスタ111、2ビットシフトレジスタ115、25ビットシフトレジスタ122、及び、20ビットシフトレジスタ123に格納される各ビットデータに、CPU103の実行する処理の内容により時間と共に変化するビットデータ、具体的には、システムバス170を通る20ビットのアドレス信号の各ビットデータA0～A19、16ビットのデータ信号の各ビットデータD0～D15、及び、その他の信号で構成される計12ビットの各ビットデータを各々加算し、加算して得られる3バイト、即ち計48ビットのデータD10～D15、D20～D215、D30～D315を乱数データとして出力する構成を採用したことを特徴とする。

【0034】上記構成を採用することで、規則性の無い予測の困難な乱数データを生成することができる。これにより、非接触ICカード100とリーダー/ライター400との間で行われる通信データを盗聴しても乱数の生成パターンを特定することが難しくなり、非接触ICカードの偽造を有効に防止することができる。また、ランダムビット生成回路110は、シフトレジスタ及び加算器(EXORゲート)を接続しただけの簡単な構成を採用するため、高速度な乱数の生成を行うことができる。

【0035】以下、ランダムビット生成回路110の構成について詳説する。ランダムビット生成回路110は、カスケード(多段直列)接続された1ビットシフトレジスタ111、2ビットシフトレジスタ115、25ビットシフトレジスタ122及び20ビットシフトレジスタ123、並びに、各シフトレジスタの出力の合計を初段の20ビットシフトレジスタ123に出力する回路を構成する3つの加算器124、125、126で構成される。

【0036】20ビットシフトレジスタ123の入力端子は加算器126の出力端子に接続される。20ビットシフトレジスタ123の出力端子は加算器126の入力端子及び25ビットシフトレジスタ122の入力端子に

接続される。25ビットシフトレジスタ122の出力端子は、加算器125の入力端子及び2ビットシフトレジスタ115の入力端子に接続される。2ビットシフトレジスタ115の出力端子は、加算器124の入力端子及び1ビットシフトレジスタ111の入力端子に接続される。1ビットシフトレジスタ111の出力端子は、加算器124の入力端子に接続される。加算器124の出力端子は加算器125の入力端子に接続される。加算器125の出力端子は加算器126の入力端子に接続される。

【0037】1ビットシフトレジスタ111は、デコード108を介してアドレス15F2Hが選択され、対応するアドレス信号線が“L”から“H”に切り換わった時に、格納する1ビットデータに、システムバス170を流れる16ビットのデータ信号のbit0のデータD0を加算して得られるデータのbit0のデータD10を乱数データとして出力する。

【0038】1ビットシフトレジスタ111は、加算器112、フリップフロップ113、トランスファゲート114で構成されている。加算器112は、例えばEXORゲートで構成され、前段に設けられる2ビットシフトレジスタ115の出力に、システムバス170を介して入力される16ビットデータ信号のbit0のデータD0を加算して得られるbit0のデータをフリップフロップ113に入力する。フリップフロップ113は、クロック同期型のフリップフロップであり、クロック入力端子に入力されるクロック信号CLKの遷移タイミングに同期して動作する。トランスファゲート114は、アドレス15F2Hが選択され、対応するアドレス信号線が“L”から“H”に切り換わった時に、フリップフロップ113の出力Qを乱数データD10として出力する。

【0039】2ビットシフトレジスタ115は、デコード108を介してアドレス15F2Hが選択され、対応するアドレス信号線が“L”から“H”に切り換わった時に、格納している2ビットの各ビットデータに、データバスを介して入力される16ビットデータ信号のbit2のデータD2及びbit1のデータD1を加算したデータD11及びD12を乱数データとして出力する。

【0040】図示するように、2ビットシフトレジスタ115は、1ビットシフトレジスタを2段直列に接続したものである。即ち、加算器116、フリップフロップ117、及び、トランスファゲート118で1つ目の1ビットシフトレジスタを構成し、次の加算器119、フリップフロップ120、及び、トランスファゲート121で2つ目の1ビットシフトレジスタを構成する。以下に説明する25ビットシフトレジスタ122及び20ビットシフトレジスタ123も同様である。各シフトレジスタ内における信号の処理内容は上記1ビットシフトレジスタ111と同様であるため、ここでの説明は省



略する。

【0041】25ビットシフトレジスタ122は、格納している25ビットの各ビットデータに、アドレスバスを介して入力される20ビットのアドレス信号のbit 0～bit 11の各ビットデータA0～A11、及び、データバスを介して入力される16ビットのデータ信号のbit 3～bit 15の各ビットデータD3～D15を加算して得られる25ビットのビットデータD<sub>13</sub>～D<sub>17</sub>、D<sub>18</sub>～D<sub>15</sub>、D<sub>20</sub>～D<sub>27</sub>及びD<sub>28</sub>～D<sub>2</sub>11を、アドレス15F2H、15F3H、15F4H及び15F5Hの選択に応じて出力する。

【0042】20ビットシフトレジスタ123は、格納されている20ビットの各ビットデータに、データ信号及びアドレス信号以外の信号で構成される8ビットの各ビットデータbit 0～bit 7の各ビットデータRev0～Rev7、及び、アドレスバスを介して入力される20ビットのアドレス信号のbit 12～bit 19の各ビットデータA12～A19を加算した20ビットのデータD<sub>212</sub>～D<sub>215</sub>、D<sub>216</sub>～D<sub>27</sub>及びD<sub>28</sub>～D<sub>215</sub>を、アドレス15F5H、15F6H及び15F7Hの選択に応じて出力する。

【0043】上述するように、ランダムビット生成回路110では、各ビットシフトレジスタ111、115、122及び123内に格納する各ビットデータに対して、システムバス170を流れるアドレス信号、データ信号及びその他の信号を構成する各ビットデータを加算する構成を採用する。システムバス170に流れる信号の値は、実行する処理内容に伴い種々変化するため、規則性の無い予測の困難な乱数データを生成することができる。これにより、非接触ICカード100とリーダ/ライタ400との間で交わされる通信データを盗聴しても乱数の生成パターンを特定することは難しくなり、非接触ICカードの偽造を有効に防止することができる。また、ランダムビット生成回路110は、シフトレジスタ及び加算器（XORゲート）を接続しただけの簡単な構成であるため、高速な乱数の生成を行うことができる。

【0044】上記ランダムビット生成回路110は、カスケード接続した全てのシフトレジスタの出力の合計を初段の20ビットシフトレジスタ123の入力端子に入力する構成を採用するが、これに限定されず、ランダムビット生成回路110を構成する4つのシフトレジスタの内の2以上のシフトレジスタの出力の合計を初段の20ビットシフトレジスタ123の入力端子に入力する構成であればよい。

【0045】また、ランダムビット生成回路110は、CPU103による所定のアドレスの選択に対応して全てのシフトレジスタに格納するビットデータを乱数データとして出力する構成を採用するが、これに限定されず、1以上のビットデータを出力する構成であればよい。

い。

【0046】更に、ランダムビット生成回路110は、各シフトレジスタに格納する全てのビットデータにシステムバス170のビットデータを加算する構成を採用しているが、これに限定されず、シフトレジスタに格納しているビットデータの内の1以上のビットデータにシステムバス170のビットデータを加算する構成であればよい。

【0047】(4-2)リセット回路

リセット回路140は、2入力NANDゲート141で構成される。NANDゲート141の入力端子にはアドレス15F1Hのアドレス信号線が接続され、残りの入力端子には書き込み命令が出た場合に“L”から“H”に切り換わるW信号線が接続されている。CPU103は、アドレス15F1Hに対してデータの書き込みを行うことで、ランダムビット生成回路110を構成する各シフトレジスタ111、115、122、123のリセットを行うことができる。

【0048】(4-3)クロック発生回路

図6に示すように、クロック発生回路130は、CLK回路131、PLL132、及び、NANDゲート133で構成される。CLK回路131は、電源回路180から電圧供給信号が出力されると同時に、所定の周期のクロック信号を基準周波数信号として次段のPLL回路132に出力する。周知のように、PLL回路132は、上記基準周波数信号の周波数に収束するまでの間、電源回路180から出力される電圧供給信号の電位に比例して決まる周波数のクロック信号を出力する。PLL回路132の出力端子は、2入力NANDゲート133の一方の入力端子に接続されている。NANDゲート133のもう一方の入力端子には、デコード後のアドレス15F0Hのbit 0のデータb0が入力される。通常、アドレス15F0Hのデータb0は“L”に設定されており、NANDゲート133は、PLL回路131からのクロック信号CLKの反転信号をランダムビット生成回路110を構成する各シフトレジスタ111、115、122及び123に出力する。

【0049】上述するように、クロック発生回路130の出力するクロック信号の周波数は、電源回路180から出力される電圧供給信号の電位により決まる。このため、電源回路180から出力される電圧供給信号の電位が規定値Vccに安定するまでの間は、全く同じタイミングで乱数データの読み取りを行っても、ランダムビット生成回路110から出力される乱数データの値は異なる。また、非接触ICカード100と全く同じ構成の非接触ICカード200や300であっても、各構成部品のばらつきにより上記乱数データの読み取りタイミングは微妙に異なるため、電源投入直後にランダムビット生成回路110から出力される乱数データは各カード毎に異なる。このように上記構成のクロック発生回路130

を採用することで、通信データの盗聴による乱数データの発生パターンの特定を一層難しくすることができ、

【0050】なお、上記構成のクロック発生回路130において、CPU103によりアドレス15F0Hのb i t 0のデータb 0が“L”から“H”に書き換えられると、NANDゲート133は“H”のみを出力する。これにより、ランダムビット生成回路110を構成する各シフトレジスタ111、115、122及び123へのクロック信号の出力は停止し、各シフトレジスタの機能は停止する。また、アドレス15F0Hのb i t 0のデータb 0の値を“H”から“L”に書き換えることで、各シフトレジスタへのクロック信号の出力を再開することができる。このように、CPU103は、ランダムビット生成回路110を動作及び停止させることができる。

【0051】(4-4)フリップフロップ  
1ビットシフトレジスタ111を構成するクロック同期型フリップフロップ113は、電源投入時に出力するデータを“H”とする第1構成要素と、上記第1構成要素と同じドライブ能力を備え、電源投入時に出力するデータを“L”とする第2構成要素を備えと共に、上記第1及び第2構成要素の出力端子に接続される配線容量を同じにしたことを特徴とする。これにより、電源投入時に出力されるデータが“H”又は“L”となる確率を50%にする。

【0052】図7は、フリップフロップ113の構成を示す図である。2入力ORゲート150の一方の入力端子は、クロック信号CLKの入力端子に接続されており、他方の入力端子はデータ信号Dの入力端子に接続されている。ORゲート150の出力端子は2入力NANDゲート151の一方の入力端子に接続されている。NANDゲート151の出力端子は、2入力NANDゲート153の一方の入力端子、ゲート電極及びソース電極が接地されているNチャンネルMOSトランジスタ159のドレイン電極、及び、2入力ANDゲート154の一方の入力端子に接続されている。2入力ORゲート152の一方の入力端子は、クロック信号CLKの入力端子に接続されており、他方の入力端子はインバータ160を介してデータ信号Dの入力端子に接続されている。ORゲート152の出力端子は、2入力NANDゲート153の一方の入力端子に接続されている。NANDゲート153の出力端子は、NANDゲート151の残りの入力端子、NチャンネルMOSトランジスタ158のドレイン電極、及び、2入力ANDゲート156の一方の入力端子に接続される。NチャンネルMOSトランジスタ158のゲート電極にはリセット端子が接続されている。NORゲート155の出力端子は、データQの出力端子、及び、NORゲート157の入力端子に接続される。NORゲート157の出力端子は、データQの反転信号QBの出力端子、及び、NORゲート155の入

力端子に接続される。

【0053】上記構成のフリップフロップ113において、電源投入時に出力するデータの値に影響を与える構成要素であるNANDゲート151及び153は、同一のドライブ能力のものを採用する。また、当該NANDゲート151と153の出力端子に接続される配線容量が同一となるように、NANDゲート151と153の出力端子に接続される配線長を同一に設計すると共に、リセット端子の接続されるNチャンネルMOSトランジスタ158により配線に付加される容量を補償するためMOSトランジスタ158と同一規格のMOSトランジスタ159を対応箇所に設ける。これにより、電源投入時にフリップフロップ113から出力端子Dに出力される信号の値が“H”又は“L”である確率を50%にすることができる。

【0054】ランダムビット生成回路110では、上記フリップフロップ113と同じ構成のフリップフロップを2ビットシフトレジスタ115、25ビットシフトレジスタ122及び20ビットシフトレジスタ123にも採用する。これにより、非接触ICカード100の起動時に各シフトレジスタから順の無い初期値が出力されるため、乱数データの予測を一層難しくすることができる。

【0055】(5)乱数生成処理  
以下、上記構成の乱数生成回路110を用いてCPU103の実行する乱数生成処理の内容について説明する。図8は、乱数生成処理のフローチャートである。まず、アドレス15F0Hのb i t 0のデータb 0を“0”にセットする(ステップS5)。これにより、クロック発生回路130からのクロック信号CLKの出力が停止し、これに伴いランダムビット生成回路110の動作が停止する。アドレス15F2H〜15F7Hを選択し、対応するアドレス信号線を“L”から“H”に切り換え、データD<sub>0</sub>0〜D<sub>1</sub>15、D<sub>2</sub>0〜D<sub>3</sub>15、D<sub>4</sub>0〜D<sub>5</sub>15を乱数データとして読み出す(ステップS6)。更に別の乱数が必要な場合(ステップS7でYES)、アドレス15F0Hのb i t 0のデータb 0を“1”にセットして、ランダムビット生成回路110を起動させた後に(ステップS8)、上記ステップS5に戻る。これ以上の乱数が不要の場合には(ステップS7でNO)、処理を終了する。上記乱数生成処理を実行することで、CPU103は、乱数生成回路110において所定のタイミングで生成された乱数データを抽出することができる。

【0056】(6)テスト処理  
上述するように、乱数生成回路107は、システムバス170を流れるデータを利用して規則性の無い予測の困難な乱数を生産することを特徴とする。ところで、所定の周波数のクロック信号CLKが入力されている状態において、ランダムビット生成回路110をリセットした

後に、非接触ICカード100のテスト処理を実行した場合を想定する。回路が正常な場合には、テスト処理の実行直後にランダムビット生成回路110から出力される乱数データは常に一定の値となる。当該特性を利用すれば、乱数生成回路107を非接触ICカード100の動作テスト装置として利用することができる。乱数生成回路107をテスト装置として利用することで、テスト専用の回路を不要にして非接触ICカード100の小型化を図ることができる。

【0057】図9は、CPU103がランダムビット生成回路110を利用して行うテスト処理のフローチャートである。まず、クロック発生回路130のPLL回路133に電源回路180から供給される電圧供給信号の電位が規定電圧Vccに安定し、所定の周波数のクロック信号CLKが安定して出力される状態で、アドレス15F0Hのビット0のデータb0を“0”にセットして、クロック発生回路130の動作を停止、即ち、ランダムビット回路110の動作を停止する(ステップS10)。アドレス15F1Hにダミーデータを書き込み、書き込み命令Wの値を“L”から“H”に切り換え、リセット回路140を機能して各シフトレジスタ111、115、122、123内のデータ(アドレス15F2H~15F7Hのデータ)をクリアする(ステップS11)。15F0Hのビット0のデータb0を“1”にセットして、クロック発生回路130を始動させる(ステップS12)。ROM104に記憶するテスト用プログラムの実行完了(ステップS13)。テスト用プログラムの実行完了後、アドレス15F0Hのビット0のデータb0を“0”にセットし、クロック発生回路130の動作を停止する(ステップS14)。アドレス15F2H~15F7Hを選択して対応するアドレス信号線“L”から“H”に切り換え、各ビットデータD<sub>1</sub>0~D<sub>1</sub>15、D<sub>2</sub>0~D<sub>2</sub>15、D<sub>3</sub>0~D<sub>3</sub>15を読み出す(ステップS15)。

【0058】内部の回路が正常の場合、上記ステップS15において読み出した各ビットデータD<sub>1</sub>0~D<sub>1</sub>15、D<sub>2</sub>0~D<sub>2</sub>15、D<sub>3</sub>0~D<sub>3</sub>15の値は一定の値を示す。そこで、上記ステップS15で読み出した各ビットデータの値と各ビットデータの基準値、例えば、前回読み出した各ビットデータの値又は予め記憶している各ビットデータの値との比較を行い、回路内部に何等かの不都合が生じているか否かの判断を行う(ステップS16)。比較の結果、上記読み出した各ビットデータの値が基準値と同じ場合には正常であると判断して処理を終了する(ステップS16でYES)。一方、上記読み出した各ビットデータが1つでも基準値と異なる場合には回路内に異常があると判断し(ステップS16でNO)、内部データの保護等の異常対策処理(ステップS17)を実行した後に処理を終了する。

【0059】以上に説明するように、乱数生成回路10

7は、システムバス170を介して入力されるアドレス信号、データ信号などの各ビットデータの値を利用して乱数生成するため、規則性の無い予測の困難な乱数データを生成することができる。また、シフトレジスタと加算器からなる簡単な構成のランダムビット生成回路110を採用することで、回路の小型化、及び、高速な乱数生成を実現する。更に、上記ランダムビット生成回路110を非接触ICカード100のテスト装置として利用することで、専用のテスト回路を排除し、非接触ICカード100の小型化を図ることができる。

【0060】なお、リード/ライト400は、非接触ICカード100の備える乱数生成回路107と同じ構成の乱数生成回路407を備える。このため、リード/ライト400でも上記非接触ICカード100と同様に、規則性の無い予測の困難な乱数データを迅速に生成することができる。更に、乱数生成回路407の備えるランダムビット生成回路(図示せず)をリード/ライト400のテスト装置として利用することで、専用のテスト回路を排除し、リード/ライト400の小型化を図ることができる。

#### 【0061】

【発明の効果】本発明の第1の乱数生成回路は、外部信号線に流れるビットデータを利用して乱数データを生成するため、規則性の無い予測の困難な乱数データを生成することができる。また、当該乱数生成回路は、シフトレジスタをカスケード接続してなる簡単な構成であるため、高速な乱数データの生成が可能である。

【0062】本発明の第2の乱数生成回路では、クロック発生回路に、基準周波数信号と同じ周波数に収束するまでの間、供給される電源電圧の値により決まる周波数のクロック信号を出力するPLL回路を用いることで、例えば、当該第2の乱数生成回路を内蔵する非接触ICカードでも、各構成部品のばらつき等により電源供給開始直後に出力される乱数データの値を相異させることができる。

【0063】本発明の第3の乱数生成回路は、上記第1又は第2の乱数生成回路において、更に、各シフトレジスタを構成するクロック同期型フリップフロップの電源投入時に出力するデータを“H”とする第1構成要素と、“L”とする第2構成要素のドライブ能力を同じにし、かつ、上記第1及び第2構成要素の出力端子に同じ容量の配線及びトランジスタを接続したことで、電源投入時に出力されるデータが“H”又は“L”である確率を50%にすることができる。これにより、電源の投入時、各シフトレジスタから偏りの無い初期値が出力され、乱数データの予測を一層難しくすることができる。

【0064】本発明の第4の乱数生成回路は、上記何れかの乱数生成回路において、更に、必要に応じて、クロック信号の出力を停止又は動作させることができる。これにより、所定のタイミングの乱数データの読み取りが

可能になる。また、必要に応じて各シフトレジスタに格納するビットデータをリセットすることができる。

【0065】本発明の非接触ICカードは、上記何れかの乱数生成回路を備えることで、規則性の無い予測の困難な乱数データを迅速に取得できるため、対応するリーダー/ライターとの間で高速な通信処理を行うことができる。

【0066】本発明のリーダー/ライターは、上記何れかの乱数生成回路を備えることで、規則性の無い予測の困難な乱数データを迅速に取得できるため、対応する非接触ICカードとの間で高速な通信処理を行うことができる。

【0067】上記第4の乱数生成回路をテスト装置として利用する本発明のテスト方法を採用すれば、テスト専用の回路が不要となり装置の小型化を図ることができる。

【図面の簡単な説明】

【図1】 リーダー/ライターと非接触ICカードの利用形態を説明するための図である。

【図2】 リーダー/ライター及び非接触ICカードとの間で実行される相互認証処理のシーケンスを示す図である。

【図3】 リーダー/ライター及び非接触ICカードのプロック構成図である。

【図4】 電源回路の構成図である。

【図5】 電源回路の出力特性を示すグラフである。

【図6】 ランダムビット生成回路の構成図である。

【図7】 クロック同期型のフリップフロップの構成図である。

【図8】 CPUの実行する乱数生成処理のフローチャートである。

【図9】 CPUの実行するテスト処理のフローチャートである。

【図10】 従来の乱数生成回路の構成図である。

【符号の説明】

100, 200, 300 非接触ICカード、101, 401 アンテナ、102, 402 送受信回路、103, 403 CPU、104, 404 ROM、105, 405 RAM、106 情報記録部、107, 407 乱数生成回路、108 電源回路、111 1ビットシフトレジスタ、112, 116, 119, 124, 125, 126 加算器、113, 120, 117 フリップフロップ、114, 118, 121 トランスファーマーゲート、115 2ビットシフトレジスタ、122 25ビットシフトレジスタ、123 20ビットシフトレジスタ、130 クロック発生回路、131 クロック回路、132 PLL回路、133 NANDゲート、140 リセット回路、141 NANDゲート、150, 152 ORゲート、151, 153 NANDゲート、154, 156 ANDゲート、155, 157 NORゲート、158, 159 トランジスタ、170 システムバス、400 リーダー/ライター、406 インターフェース

【図1】



【図2】

リーダー・ライター400の処理

ステップ1: 認証用乱数aをICカードに送信

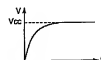
非接触ICカード100の処理

ステップ2: 暗号化鍵によりaをAに変換しAと認証用乱数bをリーダー・ライターに送信

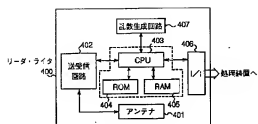
ステップ3: Aを認証し、ICカードを認証する。暗号化鍵によりbをBに変換しBをICカードに送信

ステップ4: Bを認証し、リーダー・ライターを認証する

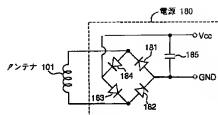
【図5】



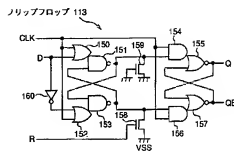
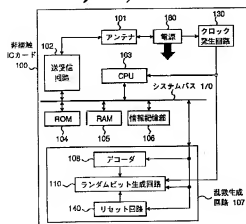
【図3】



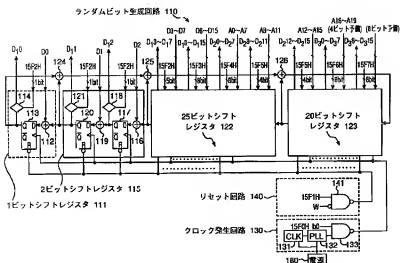
【図4】



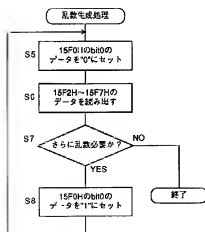
【図7】



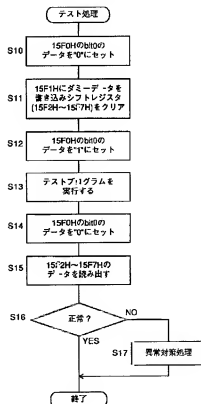
【図6】



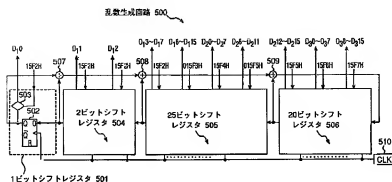
【図8】



【図9】



【図10】



フロントページの続き

F ターム(参考) 5B035 AA00 AA02 AA03 AA04 AA13  
BB09 BC02 BC03 CA01 CA08  
CA11 CA12 CA22 CA23  
5B058 CA17 CA22 CA27 KA08 KA13  
KA35 YA06 YA07  
5J104 AA18 AA41 FA04 NA23 NA35  
9A001 GG22 LL05